NAVAL POSTGRADUATE SCHOOL
MONTEREY, CALIFORNIA

THESIS

EVOLUTIONARY DESIGN OF LOCAL AREA NETWORKS

by

Ta Hsing

September 1996

Principal Advisor: Suresh Sridhar
Associate Advisor: Rex Buddenberg

Approved for public release; distribution is unlimited.

REPORT DOCUMENTATION PAGE

Form Approved OMB No. 0704-0188

1. AGENCY USE ONLY *(Leave blank)*	2. REPORT DATE	3. REPORT TYPE AND DATES COVERED
	September 1996	Master's Thesis

4. TITLE AND SUBTITLE EVOLUTIONARY DESIGN OF LOCAL AREA NETWORKS	5. FUNDING NUMBERS
6. AUTHOR(S) Ta Hsing	
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Naval Postgraduate School Monterey, CA 93943-5000	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSORING/MONITORING AGENCY REPORT NUMBER

11. SUPPLEMENTARY NOTES The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government.

12a. DISTRIBUTION/AVAILABILITY STATEMENT	12b. DISTRIBUTION CODE
Approved for public release; distribution is unlimited.	

13. ABSTRACT *(maximum 200 words)*

This study presents the evolutionary design of a local area network. In the last few years network managers have been faced with rapidly advancing technology and increased demand on LAN bandwidth from users. The purpose of this study is to assist network managers in decision making when developing a mid-size LAN.

The methodology for this study is to develop a mid-size LAN using current technology to replace a router-based design with a switch-centric design. As an example, the current proposal for the ROC military school's campus network is used as a basis for redesigning a LAN by taking advantage of the emerging switch technology. This switch-centric design is evolved from a revised basic model to an enhanced and advanced model.

The resultant design arrived at is less expensive, easier to manage, and simpler than the current router-based design and allows greater flexibility to meet user's increasing bandwidth demands. The fundamental advantages of switching technology over router based solutions is a lower per port cost, higher capacity and faster response.

14. SUBJECT TERMS LAN Design			15. NUMBER OF PAGES 76
			16. PRICE CODE
17. SECURITY CLASSIFICATION OF REPORT Unclassified	18. SECURITY CLASSIFICATION OF THIS PAGE Unclassified	19. SECURITY CLASSIFICATION OF ABSTRACT Unclassified	20. LIMITATION OF ABSTRACT UL

NSN 7540-01-280-5500

Standard Form 298 (Rev. 2-89)
Prescribed by ANSI Std. 239-18 298-102

Approved for public release; distribution is unlimited.

EVOLUTIONARY DESIGN OF LOCAL AREA NETWORKS

Ta Hsing
Major, Republic of China Marine Corps
Chinese Naval Academy, 1982

Submitted in partial fulfillment
of the requirements for the degree of

MASTER OF SCIENCE
IN
INFORMATION TECHNOLOGY MANAGEMENT

from the

NAVAL POSTGRADUATE SCHOOL
September 1996

Author: _____
Ta Hsing

Approved by: _____
Suresh Sridhar, Principal Advisor

_____
Rex Buddenberg, Associate Advisor

_____
Reuben T. Harris, Chairman
Department of System Management

ABSTRACT

This study presents the evolutionary design of a local area network. In the last few years network managers have been faced with rapidly advancing technology and increased demand on LAN bandwidth from users. The purpose of this study is to assist network managers in decision making when developing a mid-size LAN.

The methodology for this study is to develop a mid-size LAN using current technology to replace a router-based design with a switch-centric design. As an example, the current proposal for the ROC military school's campus network is used as a basis for redesigning a LAN by taking advantage of the emerging switch technology. This switch-centric design is evolved from a revised basic model to an enhanced and advanced model.

The resultant design arrived at is less expensive, easier to manage, and simpler than the current router-based design and allows greater flexibility to meet user's increasing bandwidth demands. The fundamental advantages of switching technology over router based solutions is a lower per port cost, higher capacity and faster response.

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

I. INTRODUCTION

A. PURPOSE OF THIS RESEARCH

A year ago, network managers faced a dilemma when both the Fast Ethernet (100BASE-T) and 100VG-AnyLAN were introduced into the market. They did not know which technology to select in order to maximize network performance amidst ever-growing bandwidth demands.

The purpose of this research is to present an overview of existing network technologies including their merits and demerits. Additionally, this study will describe a development strategy for implementing these new technologies and demonstrate a graceful networking evolution in support of the typical organizational goals of increased productivity and high quality.

B. METHODOLOGY

The methodology for this research includes a survey of the existing literature on network technology and browsing the Internet for the latest information in this rapidly evolving field. Personal experience in the design and implementation of a network for San Benancio Middle School was applied to this research. Additionally, information from interviews with the technicians who maintained the network in Ingersoll Hall at the Naval Postgraduate School was used. To demonstrate a graceful evolution of a network, the study uses the proposed network design for the Chinese military schools as a basic system to be revised and redeveloped.

C. SCOPE

This research focuses on LAN technologies. The research encompasses characteristics of network components to LAN architecture and introduces the logic scheme and considerations for network planning and development. The size of networks considered for an organization is usually in the range of 200 to 400 users. This research does not go

into any depth of detail in the techniques of economic analysis and the provisioning process for networks.

D. BENEFITS

This study may provide CIO or upper management with a better picture of how the organization's network may grow and assist him in providing appropriate support to his organization. Additionally, the study may assist a network manager to plan for network upgrade. The study will use the current Chinese military schools network proposal as an example for the redesign of a midsize network with the more appropriate technology of switching.

E. ORGANIZATION OF THIS STUDY

This chapter has been an introduction to the study. Chapter II presents an overview of network technologies. Chapter III presents a brief introduction to the design of a network. Chapter IV uses the basic model of the Chinese military school's network as an example and develops a better design based on switching technology. Chapter V demonstrates the evolution of the revised model presented in Chapter IV. Chapter VI presents conclusions and recommendations of this study.

II. OVERVIEW OF NETWORK TECHNOLOGIES

A. BACKGROUND

Networks are made up of three components: media, protocols, and nodes.

- Media provide path ways for data to travel between nodes in the network, it may be metallic cable, fiber-optic, or wireless.
- A protocol is a set of predefined rules that govern how two or more processes communicate and interact to exchange data.
- Nodes are the place for input or output of data in a network, it may be a PC, terminal, workstation, printer, even a mainframe.

1. Media

a. Cable

Cables are currently the most popular medium for transmission of data between the nodes of a network. There are three types of cable: twisted-pairs, coaxial and fiber-optic. (See Figure 1)

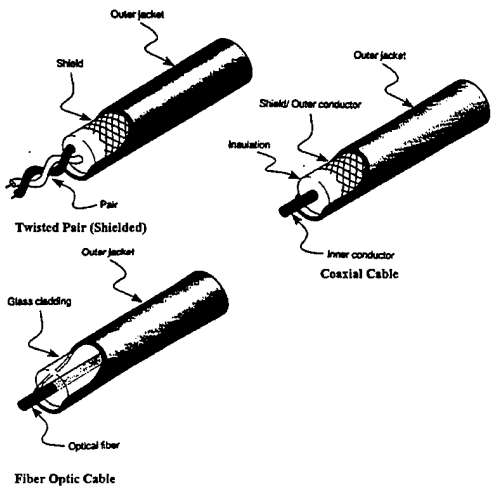

Figure 1. Cable Media
From Ref. [1, pp. 543-545]

(1) Twisted-pair Cable. Consists of two insulated copper wires twisted together in a helical form and covered by a common insulated sleeve. The twisted form is used to reduce radio and electrical interference. The greater the number of twists in a pair the less interference. Twisted-pair may be unshielded as is the case of regular telephone line, or shielded with braiding or foil. The Electrical Industries Association divides Unshielded Twisted-pair (UTP) into different categories by grade. The rating for each category refers to conductor size, electrical characteristics, and twist per foot. Table 1 summarizes the UTP categories.

Category	Capacity(Mbps)	Usage
1 and 2(voice grade)	<4	older telephone line
3	<16	most currently phone line
4	<20	10 base-T , Token-Ring
5	<100	Fast Ethernet, 10 base-T

Table 1. Unshielded Twisted-Pairs Cable Categories

Although many networks now use UTP, Shielded Twisted-pair (STP) is still used. The STP cable is less vulnerable to electrical interference than UTP. IBM has its own specifications for different qualities and configurations of STP. See Appendix A (IBM Cable System) and Table 2 for the characteristic of cable.

Factor	**UTP**	**STP**	**Coaxial**	**Fiber-Optic**
Cost	Lowest	Moderate	Moderate	Highest
Installation	Easy	Fairly easy	Fairly easy	Difficult
Capacity	1 to 100 Mbps (typically 10 Mbps)	1 to 155 Mbps (typically 16 Mbps)	Typically 10 Mbps	2 Gbps (typically 100 Mbps)
Attenuation	High (range of hundreds of meters)	High (range of hundreds of meters)	Lower (range of a few kilometers)	Lowest (range of tens of kilometers)
EMI	Most sensitive to EMI and eavesdropping	Less sensitive than UTP but still sensitive to EMI and eavesdropping	Less sensitive than UTP but still sensitive to EMI and eavesdropping	Not affected by EMI or eavesdropping

Table 2. Characteristics of Cable Media
From Ref [2, p. 899]

(2) Coaxial Cable. Coax has two conductors that share the same axis. At center of cable is a solid copper conductor surrounded by a plastic insulator. A wire mesh tube and metallic foil, the second conductor encloses the insulator to protect the wire from Electromagnetic Interference (EMI). The outest is a tough plastic cover providing protection and insulation.

Coax is classified by size and its resistance. The following are commonly used in networking: [Ref. 2, p. 905]

- 50 ohm, RG-8 and RG-11, used for Thick Ethernet
- 50 ohm, RG-58, used for Thin Ethernet
- 75 ohm, RG-62, used for cable TV

(3) Fiber-optic Cable. Fiber-optic cable transmits light signals rather than electrical. It is enormously more efficient than the other media in terms of bandwidth and distance. It is also immune to eavesdropping.

Each optical fiber consists of an extremely thin fiber of glass or fused silica, called a "core" that conducts light and is surrounded by concentric layers of glass known as "cladding". The outermost layer surrounding one fiber or a bundle of cladded fibers, is the protective sheath.

Optical fiber may be classified as single-mode or multimode. Single-mode fiber has a single light path which is used with laser signaling up to 20 km. Single-mode has greater bandwidth and a longer distance for data transmission but is more expensive than multimode. Multimode allows transmission of typically 2 km. The following are the common types of fiber optic cables for networking:

- 8.3 micron core/125 micron cladding, single mode,
- 62.5 micron core/125 micron cladding, multimode,
- 100 micron core/140 micron cladding, multimode.

b. Wireless

Wireless transmission medium rely on electromagnetic spectrum to carry data instead of cable. Wireless networks are categorized as radio wave, microwave, and infrared network according to frequencies they use. See Figure 2. The Electromagnetic Spectrum [Ref. 3, p. 69]. Wireless networks are used for the following purposes:

- Overcoming obstacles that cable cannot reach.
- Connecting machines within a building.
- Connecting portable or mobile machines to a network.
- Keeping a mobile machine in contact with a database.
- Ad hoc networks (for example, in committee or business meetings). [Ref. 4, p. 682]

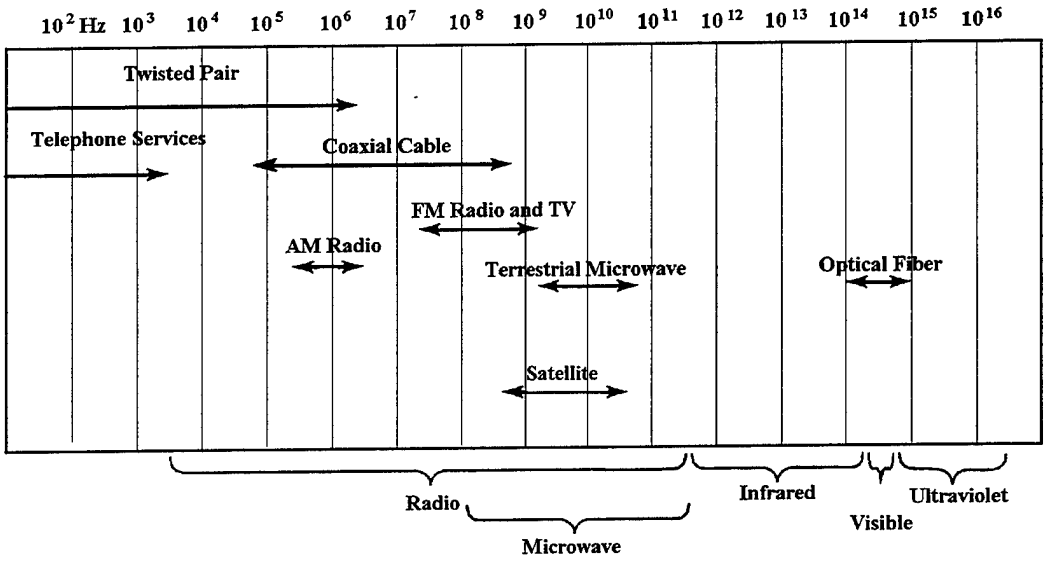

Figure 2. The Electromagnetic Spectrum

(1) Radio Wave. Radio wave systems operates at frequencies from a few megahertz (MHz) to about 3 gigahertz (GHz).They use either a single-frequency (base band) or spread-spectrum (broad band) transmission technology. A base band transmits within a single, generally small, frequency band. Base band is susceptible to eavesdropping,

interference, and jamming. In contrast, a broad band distributes the transmission across a broader frequency range. The "spreading" sequence may be determined at random, and must be known to the receiver. This technology is difficult to intercept without knowing the spreading sequence, and is unlikely to be interfered with by other transmissions. [Ref. 4, p. 683]

(2) Microwave. Microwave communication make use of the lower gigahertz frequencies of the electromagnetic spectrum. These frequencies are higher than radio frequencies and produce higher throughput and performance. Microwave communication use either an earth-based antenna or a satellite in geosynchronous orbit as the retransmission point. The signals are highly focused and the physical path must be line-of-sight. With a satellite, the signal can be transmitted thousands of miles; with earth-based antennas, the signal is limited to a few kilometers. Microwave transmissions are susceptible to eavesdropping, jamming, and interference.

(3) Infrared. Infrared networks use frequencies ranging from a few hundred GHz to about 1 terahertz (THz), just below the visible light spectrum.

These waves require a line-of-sight connection between sender and receiver or between each of these and a common cell. An infrared signal can be focused or diffused. A focused signal is aimed directly at the target (receiver or cell), or the signal may be beamed at a surface and reflected off this to a receiver. This focused type of signal can travel over a greater range but only to a specific target. In contrast, a diffuse signal travels in multiple directions, but is much weaker than a focused signal in any one direction. As a result, the range of a diffuse signal is much shorter than for a focused signal. [Ref. 4, p. 683]

Infrared transmissions have very high bandwidths and may be in a range above 400 gigahertz to 1 terahertz. Infrared signals are vulnerable to natural conditions such as rain and fog, and there is a health risk from infrared radiation.

2. Protocols

A protocol is a set of predefined rules that govern how two or more processes communicate and interact to exchange data. The processes can be on the same machine or

on different machines. For example, a transport-layer program on one machine uses a protocol to talk to the program's counterpart on another machine. Protocols are generally associated with particular services or tasks, such as data packaging or packet routing. A protocol specifies rules for setting up, carrying out, and terminating a communications connection. Protocols also specifies the format the information packets must have when traveling across this connection.

3. Networks Topology

Network topology has two aspects: Physical and logical. Physical topology specifies how network devices are linked. Logical topology specifies how the messages travel on a network. The following is a discussion of different physical topologies.

a. Ring

A ring topology connects all the nodes with one continuous loop. Within this loop the data travels in one direction only, making a complete circle around the loop.

Advantages:

- The cable requirements are fairly minimal, and no wiring center or closet is required.

Disadvantages:

- If any node goes down, the entire ring goes down.
- Diagnosis/troubleshooting (fault isolation) is difficult because communication is only one-way.
- Adding or removing nodes disrupts the network.

b. Bus

In a bus topology each of the nodes is connected to the single cable that runs the entire length of the network.

Advantages:

- Architectures based on this topology are simple and flexible.
- A bus uses relatively little cable compared to other topologies.
- It's easy to add or remove nodes from the bus.

Disadvantages:

- Diagnosis/troubleshooting (fault-isolation) can be difficult.
- The bus trunk can become a bottleneck when network traffic gets heavy.

c. Star

A star topology connects all the nodes to the central component (generally known as a hub), each with its own data circuit. [Ref. 4, p. 1002]

Advantage:

- Troubleshooting and fault isolation are easy.
- Easy to add or remove nodes.
- Easy to modify the cable layout.

Disadvantage:

- If the hub fails, the entire network fails.
- A star topology requires a lot of cable.

d. Tree

A tree topology is a hybrid topology that combines features of star and bus topologies. Several buses may be daisy-chained together, and they may branch at the connections (which will be hubs).

Advantages:

- Network is easy to extend by just adding another branch.
- Fault isolation is relatively easy.

Disadvantages:

- If the root (starting end) goes down, the entire network goes down.
- If any hub goes down, all branches off that hub go down.
- Access becomes a problem if the entire conglomerate of buses becomes too large.

e. Mesh

A mesh topology is a topology in which there are at least two paths to and from every node.

Advantages:

- It has robust defenses against node or link failure. If a connection is broken in this layout, at least one substitute path is always available.

Disadvantages:

- It is complex and very expensive to build.

4. Network Modeling

Nodes on a network can be servers or workstations. A workstation makes requests, and a server fulfills them. Networks can be classified by relationships among nodes such as Peer-to-peer, Distributed, Server-based, and Client/server network. The peer-to-peer and client/server networks have gained popularity.

a. Peer-to-peer Networking

In a peer network every node can be both client and server; that is, all nodes are equal. Each node can initiate actions, access other nodes, and provide services for other

nodes without requiring a server's permission, although access or password restrictions may be in effect.

Advantages:

- It is simple and cheap, a natural for small business.
- It mirrors the way people really work, and tends to foster collaboration and improve workflow.
- There is no dedicated LAN administrator or special training needed.

Disadvantages:

- There are inadequate security and backup features.
- It tends to have traffic and resource congestion.

Most of the high-end 32-bit "server NOS" are technically peer-to-peer as well, including LAN Server, LAN Manager and NT. Peer-to-Peer is now just another feature.

b. Client/Server Computing

The Client/server computing is a sophisticated version of a server-based network. While workstations in a server-based network may have access to all sorts of resources through the server, the workstation must do most of the work. The server downloads files and, possibly, applications to the workstation, and then lets the workstation run the programs.

In the most general form of client/server computing, the workstation makes a query or request, and the server processes the query or request and returns the results to the workstation.

The ideal network is a combination of network types. The peer aspect lets you exchange files without server intervention, as well as easily set up dynamic work groups. Server-centric aspect takes care of file and print management tasks and high-end communications.

B. INTERNETWORKING

1. Interoperability:

Many different communication systems and equipment combinations are used throughout the world. This has created the need for a common language that allows different types of computers to communicate and to transfer data between them.

Various models have been proposed for network management. The two most comprehensive proposals are the models developed for the International Standards Organization (ISO) seven-layer Open Systems Interconnection (OSI) model and for the Internet Protocol (IP, or TCP/IP).

a. OSI Model

The OSI model is a standard that outlines how to connect any combination of devices for purposes of communications. The OSI model is nothing tangible; it is simply a conceptual framework which can be used to better understand the complex interactions taking place among the various devices on a network.

This model describes the task in terms of seven functional layers, and specifies the functions that must be available at each layer. The focus in this model is on the "interconnection" and on the information that can be passed over this connection. [Ref. 2, p. 1124]

The best way to understand this model is to combine the seven layers into "macro-layers." The top three layers, Application, Presentation, and Session, focus on user applications. The next two layers, Transport and Network, deal with the logical issue of transmission. The bottom layers, Data Link and Physical handle the physical transmission of data. See Figure 3 for the macro layer's, and Appendix E for a description of the OSI reference model.

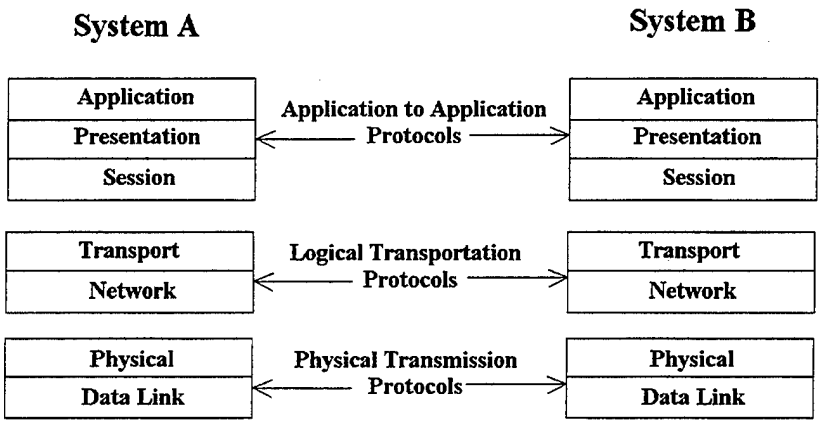

Figure 3. The OSI Model

b. TCP/IP Protocol Suite

The Transmission Control Protocol/Internet Protocol (TCP/IP) is a product of common effort of several U.S. government agencies joined with major universities and corporate researchers. TCP/IP makes heterogeneous network systems communication possible and easy. During the 1980s, TCP/IP became a requirement in many U.S. government bids. This caused many vendors to add TCP/IP to their products. All this activity, combined with the growth in UNIX and easy to use, inexpensive software resulted in a tremendous growth in TCP/IP. [Ref. 5, p. 77].

Today, TCP/IP is a truly open standard. It is standard equipment in many operating systems, including Windows 95, NT, and UNIX.

The TCP/IP can be viewed from a conceptual model called the DoD networking model which is similar in concept to the OSI model. Yet the specifications on how those functions are to be implemented are different. Figure 4 is the TCP/IP protocol suite [Ref. 2, p. 1130]. The four layers of DOD model are:

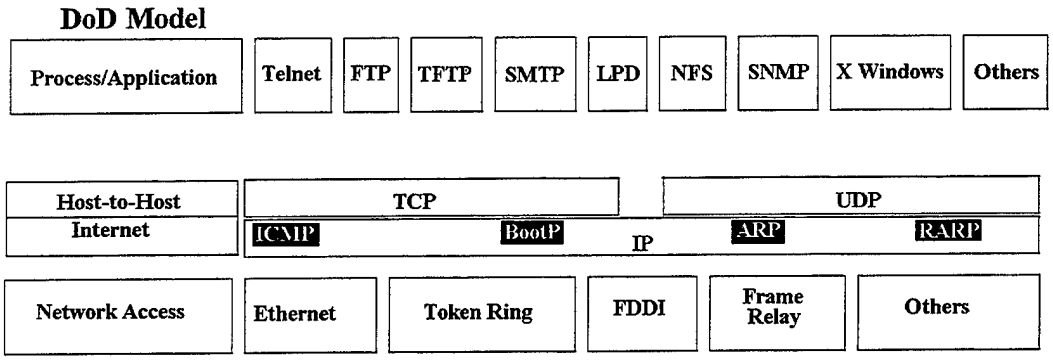

Figure 4. TCP/IP Protocol Suite

(1) Process/Application Layer. Defines protocols for host-to-host application communication. It also controls user interface specifications. These common use applications include File Transfer Protocol (FTP) for moving files among computers; Telnet for generic, remote log-in to another host; Simple Mail Transfer Protocol (SMTP) for electrical mail; Simple Network Management Protocol (SNMP) for network management.

(2) Host-to-Host Layer. Defines protocols for setting up the level of transmission service for the communication. In this layer Transmission Control Protocol (TCP) is a full-duplex, connection-oriented protocol providing reliable end-to-end communication between nodes. TCP sets up and terminates connections, imposes flow control, provides error correction, and guarantees that data is delivered reliably to the upper layer user. Another exclusive protocol to TCP is Datagram Protocol (UDP) which is used for transaction-oriented application.

(3) Internet Layer. Defines protocols relating to the logical transmission of packets over the entire network. IP provides a connectionless datagrams delivery service. It links subnetworks into internetwork via gateways that route IP packets between the subnetworks. IP does not provide reliable data transfer, it uses "best effort" to deliver datagrams.

(4) Network Access Layer. Defines protocols for the physical transmission of data. Some of the technologies that implement this layer are Ethernet, Token Ring and FDDI which will be addressed in next chapter.

2. Connectivity

a. Repeater

A Repeater is a hardware device that functions at the physical layer of the OSI model and is used to connect two segments of the same network.

A repeater moves all packets from one network segment to another by regenerating, retiming, and amplifying the electrical signals. The main purpose of a repeater is to extend the length of the network transmission medium beyond the normal maximum cable lengths.

It is important to note that a repeater can increase segment length only to overcome electrical restrictions; the repeater cannot be used to increase the time limitations inherent in the network's layout. For example, a repeater cannot stretch the network so that a transmission could take more than the allowable slot time to reach all the nodes in an Ethernet network. The IEEE specifications allow no more than four repeaters in a series between two nodes in an Ethernet network. [Ref. 4, p. 827]

Multiport repeaters connect several segments. These repeaters generally have an autopartitioning capability, which allows them to disconnect any faulty segments automatically. This effectively quarantines the segment with the faulty node.

b. Bridge

Bridges operate at layer 2 of OSI model. Bridges can pass packets from one network to another. A bridge serves both as a medium and a filter. It allows packets to be sent to a node on another network. At the same time, the bridge discards any packets intended for the originating network rather than passing these to the other network. A bridge reduces traffic on both networks by protecting each network from the other network's local messages. This makes each of the smaller networks faster, more reliable, and more secure.

A bridge is independent of higher level protocols. Different higher level protocols can use the same bridge to send messages to other networks. Networks connected by a bridge can be treated as part of the same logical network. There are two types of bridges, the MAC-layer and LLC-layer bridge.

MAC-layer bridges operate at the lower sublayer of data-link layer. These bridges can connect only networks using the same architecture (Ethernet to Ethernet, Token Ring to Token Ring, and so on), because the bridge expects to handle a particular packet format, such as Ethernet or ARCnet.

LLC-layer bridge operate at the upper sublayer of the data-link layer. These types of bridges can connect different architectures (such as Ethernet to Token Ring), because these architectures use the same LLC sublayer format, even though they use different format at the MAC sublayer.

c. Switch

A switch is specifically designed to address LAN performance problems resulting from bandwidth shortages and network bottlenecks. A switch economically segments the network into smaller collision domains, providing a higher percentage of bandwidth to each end-station.

Switching technology operates at layer 2 of the OSI model. The emerging popularity of switching products can be viewed as a resurgence of bridge technology in a simpler, higher-performance, and higher-port-density device [Ref. 6]. Like a bridge, a switch makes a relatively simple forwarding decision based on the destination MAC address contained in each packet.

Switches solve today's critical bandwidth shortages by segmenting a repeated LAN collision domain into smaller collision domains (Figure 5). This segmentation reduces or nearly eliminates station contention for media access and provides each end-station with a larger share of the available LAN bandwidth. Also a switch enhanced network performance because layer 2 segmentation reduces the number of stations competing for media access.

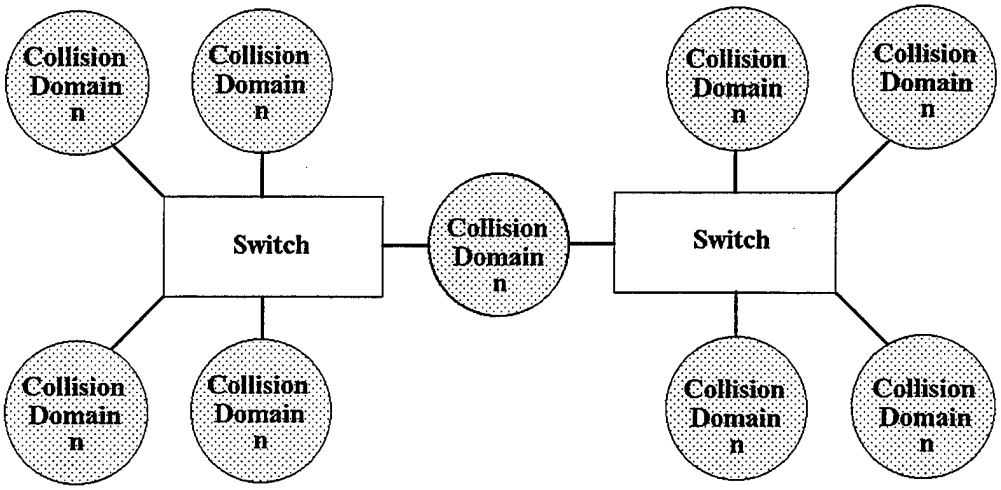

Figure 5. LAN Collision Domain Divided into Smaller Collision Domains
After Ref. [6]

It is important to note that the individual collision domains created by the switch are still members of the same broadcast domain. This means that broadcast traffic originating in one collision domain is still forwarded to all other collision domains, ensuring that all stations in the network can still communicate with one another.

d. Router

A router operates at layer 3 of the OSI model, distinguishing among network layer protocols and making intelligent packet-forwarding decisions.

One of the primary functions of a router is to provide traffic isolation to help diagnose problems. Because each port of a router is a separate subnetwork, broadcast traffic is not forwarded across the router. The definition of network boundaries makes it easier for a network manager to provide redundancy and to isolate problems resulting from broadcast storms, misconfigurations, chatty hosts, and equipment failures. [Ref. 6] Routers keep these potentially disastrous events local to the area in which they occur, preventing them from spreading across the entire network.

Routers have the ability to calculate the most efficient path across a network based on a combination of metrics such as delay, throughput, reliability, and hop count. In addition, routers may employ other methods such as "policy" to control the flow of traffic

and restrict the propagation of routing information. These abilities are most effective where WANs are used, or where multiple LAN technologies are involved.

This increased intelligence can also result in enhanced data security, improved bandwidth utilization, and allowing more control over network operations. The disadvantage is that the additional frame processing performed by a router can increase latency, reducing the network's performance when compared to a simpler switch architecture.

C. STANDARD LAN (BASIC)

1. Ethernet

Ethernet specifies a LAN operation at speeds of 10 Mbps using frames that can be carried up to 1500 bytes of user data. Ethernet 2.0 is currently the official Ethernet standard. This is also known as DIX (for Digital, Intel, Xerox) Ethernet or Blue Book Ethernet. Ethernet networks use CSMA/CD as the media access control mechanism. CSMA/CD stands for "Carrier Sense Multiple Access, with Collision Detection". It works as follows: Before an Ethernet device puts a packet "on the wire", it listens to determine if another device is already transmitting. Once the device finds the wire is clear, it starts sending the packet, while at the same time listening to hear if another device has started sending and a collision has occurred. The colliding nodes both retreat when a jamming signal from a collision is detected. Each node waits a random amount of time before trying again. If there is no collision, the frame is broadcast onto the network. All nodes listen to each packet transmitted.

A variant on this standard was formulated by the IEEE 802.3 work group. This variant is sometimes called Ethernet as well. However, although Ethernet and 802.3 are similar, there are differences in the way the data-link layer is handled and in the format of a packet.

Because of these differences, difficulties will arise if you try to mix different types of Ethernet on the same network. With a multi-flavor server, nodes that use different Ethernet versions may be able to communicate with each other, but only through the server.

For example, nodes using 802.3 and Ethernet 2 NICs may be able to pass packets, but they will not be able to communicate directly with each other.

a. Ethernet Architecture Rules

- There may be no more than five (5) repeated segments,
- No more than four (4) repeaters between any two Ethernet stations;
- Of the five cable segments, only three (3) may be populated.

This is referred to as the "5-4-3" rule (5 segments, 4 repeaters, 3 populated segments).

b. Ethernet Flavors

These are the IEEE definition for the different physical types of Ethernet. The "10" stands for signaling speed: 10MHz. "Base" means Baseband, "broad" means broadband. Initially, the last section indicates the maximum length of an unrepeated cable segment in hundreds of meters. This convention was modified with the introduction of 10BASET, where the T means twisted pair, and 10BASEF where the F means fiber. [Ref. 4, p. 345]

- 10BASE2 limited to 185 meters per unreported cable segment.
- 10BASE5 limited to 500 meters per unreported cable segment.
- 10BASEF limit depends on the signaling technology and medium used but may span up to 2KM.
- 10BASET limited to 100 meters per unreported cable segment.
- 10Broad36 limited to 3,600 meters (almost 2.25 miles).

Advantages of Ethernet

- Support from most of vendors.
- Easy to install.
- Technology is well-known and thoroughly tested.

- Moderate costs.
- Flexible cabling, especially when using twisted-pair cable.

Disadvantages of Ethernet

- Heavy traffic can slow down a network that uses CSMA/CD access system.
- Since all nodes are connected to the main cable in most Ethernet networks, a break in this cable can bring down the entire network.
- Troubleshooting is more difficult with bus topology.
- Room for incompatibilities because of frame structure (such as 802.3 versus Blue Book Ethernet)

2. Token-ring

Token Ring is a network architecture that uses a ring network topology and a token-passing strategy to control access to the network. The IEEE 802.5 standard defines the Token Ring architecture and specifies how this architecture operates. IBM has developed its own revisions. These differ somewhat from the official IEEE 802.5 specifications, but they have become so widely used that discussions of token ring generally mean IBM Token Ring.

Using token passing as the media-access method, the token is passed from node-to-node in a fixed direction around the logical ring structure. The node with the token is allowed to send a message to another node.

Token passing is deterministic. This means each node is guaranteed to get a turn sending packets within a predefined time. Although they use a logical ring structure, Token Ring networks are actually arranged in a physical star topology, with each node connected to a central hub (the MAU).

Token Ring networks have the following features:

- Operates at either 1 or 4 Mbps, for IEEE 802.5; operate at either 4 or 16 Mbps, for IBM.

- Uses baseband signaling, which means that only one signal travels along the line at a time.
- Uses shielded twisted-pair (STP) or unshielded twisted-pair (UTP) cable or fiber-optic cable, but not coaxial cable. The STP has a 150 ohm resistance, and the UTP has a 100 ohm resistance.
- Use four-wire cable, with two of the wires used for the main ring and two for the secondary.
- Has each node (called a lobe in IBM terminology) connected to a wiring center, called an MAU (multistation access unit).
- Allow MAUs to be connected to each other, to create larger rings.
- Allow the use of patch panels, which sit between nodes and MAUs and make it easier to reconfigure the network.
- Require built-in network management facilities, because nodes need to be able to determine whether a token has been corrupted, destroyed, or lost.
- Are controlled by the node that generates the token. This node (which is known as the active monitor) is generally the network file server.

Token Ring networks have two types of length restrictions: the lobe length and the ring length. The lobe length is the distance between a node and an MAU. The ring length is the distance between MAUs on the main ring path. See details APPENDIX B. Token Ring lobe length and ring length restrictions. Other restrictions on Token Ring networks include the following:

- At most three cable segments (separated by repeaters) are allowed in a series.
- Each cable segment must be terminated at both ends and grounded at one end.
- In the IEEE 802.5 specifications, a network can have up to 250 lobes.
- In the IBM Token Ring specifications, a network using STP can have up to 260 lobes; one using UTP can have up to 72 lobes.
- At most, 33 MAUs are allowed on the network.

- A network cannot have nodes operating at different speeds. That is, a network may consist of 4 Mbps or 16 Mbps lobes, but not both. You can, however, use a bridge to connect a 4 Mbps to a 16 Mbps Token Ring network.

- To operate a 16 Mbps the cable needed is at least at Category 4 (Rated to 20 MHz) in the EIA/TIA-568 classification system.

Advantages of Token Ring:

- Easy to connect to IBM mainframe-based networks.

- Guarantee each node has opportunity to transmit in a time frame.

- Performance are better than Ethernet in heavy traffic load from many users.

Disadvantages of Token Ring:

- Components are more expensive than for Ethernet.

- Token Ring architecture is not easy to extend to wide-area networks. [Ref. 4]

D. HIGH SPEED LAN

There are several factors driving the need for additional bandwidth in the LAN environment, including:

- The ever-increasing number of network nodes.

- The continuing development of faster and more powerful microprocessors for workstations and servers.

- The emergence of a new breed of bandwidth-intensive client/server applications.

- The growing trend toward the deployment of centralized server farms to ease administration and reduce the total number of servers.

1. Fast Ethernet

The 100BASE-T Fast Ethernet standard was developed as a direct extension of the popular 10BASE-T Ethernet.100BASE-T and uses the same CSMA/CD access method as 10BASE-T, and a similar star topology. However, the 100BASE-T standard incorporates

new physical-layer signaling schemes that support 100 Mbps data rates over a range of twisted-pair and fiber cabling types. To accomplish this higher throughput, the collision domain, or network diameter, had to shrink from 2,500 meters to 205 meters, and the InterFrameGap was reduced to one-tenth its original value, from 9.6 microseconds to .96 microseconds.

There are three distinct cabling variations to the 100BASE-T standard. They are as follows:

- 100BASE-TX for 2-pair data grade Category 5 UTP (unshielded twisted pair) and Type 1 STP (shielded twisted pair).
- 100BASE-T4 for 4-pair voice and data grade Category 3, 4, or 5 UTP.
- 100BASE-FX for 2 strand multimode fiber.

The 100BASE-T standard retains 10BASE-T's critical 100-meter maximum cable length between the hub and the desktop, but some 100BASE-T rules differ from 10BASE-T rules because of the increase in speed. See details APPENDIX C. 100BASE-T topology rules. [Ref. 7]

Advantages

- Cheapest technology for providing 100Mbps bandwidth.
- Provides backward support to 10BASE-T networks.
- Provides cost-effective migration from 10BASE-T.
- Nearly all vendors support 100BASE-T.

Disadvantages

- The practical bandwidth is much lower than 100Mbps (average to 40~50 Mbps) due to the collisions.
- Lacks scalability compare to 10BASE-T and other technologies.
- Inappropriate for applications where deterministic delivery is required.

2. 100VG- AnyLAN

100VG-AnyLAN is the second of two emerging standards for 100Mbps Ethernet backed primarily by Hewlett-Packard. Support for both Ethernet and token ring frame types has led to the "AnyLAN" name.

100VG-AnyLAN operates over Category 3, 4 or 5 UTP and uses an access scheme called "Demand Priority" to determine the order in which nodes share the network. 100VG-AnyLAN also allows for two levels of priority for network traffic, "normal" or "high." Demand Priority services high priority first during each "round," allowing time-critical network applications more immediate access to the network. Because all nodes requesting access are served during each "round," all nodes are assured access to the network. The following table summarizes the 100VG cabling distance.

Category	Four-Pair (UTP)	Two-Pair (STP)	Node-to-Node/Node-to-Hub
3	◊	◊	100m
4	◊	◊	100m (STP)
5	◊	Under Consideration	200m (UTP)
Fiber-Optic			2000m

Table 3. 100VG-AnyLAN Cabling Distances

100VG-AnyLAN allows a network diameter of 2,000 meters and supports cascading up to two tiers of hubs below a "root" hub.

The 10BASE-T rule of no more than four concentrators between any two nodes should be followed. There can be up to 1024 nodes on a single VG segment. However, Hewlet Packard recommends that the practical working limit is 250. [Ref. 8]

An entire VG network either uses the Ethernet frame format or Token Ring frame format. Usually, a VG network will run using the Ethernet frame format unless it is being bridged to a Token Ring network.

VG will be primarily deployed as a workgroup solution, but offers some scalability for smaller backbone applications.

Advantages:

- 100Mbps bandwidth is nearly achievable due to lack of collisions.
- Demand Priority Provides fair access to the network.
- Large topology breadth with up to five levels of cascading.
- Nodes are on one segment -- just like Ethernet and Token Ring.
- Uses major media plant to minimize cable pulling.
- Security of network increased with point-to-point links.

Disadvantages:

- All products for full enterprise network are available, yet not from more than one vendor.
- Products of all supported cable plants not available yet.
- Small community of vendors.
- Requires learning Demand Priority Protocol.

a. Typical Applications

Not all applications on networks will see significant benefits from the use of Demand Priority. However, the typical applications that stand to gain the most in terms of increased performance due to increased access to the media include the following applications:

- Multimedia Applications
- Desktop Video Conferencing
- Video-on-Demand
- Desktop Imaging
- Secure Network Configuration

3. FDDI

FDDI is a 100Mbps network technology based on a timed token passing access method. Standardized by ANSI, FDDI uses a ring or star wired ring topology using fiber-optic or copper media. FDDI was designed to operate as a high-speed backbone technology and contains several elements to enhance its capability in backbone environments. This includes a capability for dual counter-rotating rings, which provide a redundant data path in the event of a cable failure; and extensive management support built into the protocol. In recent years, support for STP and UTP cable has been added to the specification to enhance its capabilities as a workgroup solution.

FDDI allows a maximum network length of 200 kilometers and provides for up to 500 stations on a single ring. FDDI nodes can be either "dual attached" or "single attached." Dual attached stations allow connection to both counter rotating rings and are usually used by network hubs or server adapters. Single attached nodes are usually based on STP or UTP cable and allow connection to an FDDI concentrator.

Advantages:

- FDDI enjoys strong industry support as a backbone solution. Its high speed, combined with its large data frame size, enhance its acceptability for backbone applications.
- Its dual-ring architecture provides a high level of fault tolerance for mission-critical backbone environments.
- Its token-based access method provides deterministic performance.
- It offers a larger network diameter than other available 100Mbps options.

Disadvantage:

- FDDI is a degree of magnitude more expensive than other high-speed options.
- FDDI is considered difficult to install, and the additional overhead associated with station management minimizes FDDI's cost effectiveness to the desktop. [Ref. 9]

- Complexity: Scaling the network will result in large numbers of routers/router ports, each (potentially) with its own subnet address. Large number of devices and address administration may become burden to manager.

- Hops between routers and across shared-access Ethernet and FDDI LANs may hurt application performance. Problems are exacerbated if backbone needs to be segmented to carry more traffic.

4. ATM

Asynchronous Transfer Mode (ATM) is an evolving network standard initially proposed for wide area networking and has also been promoted for use in LANs. Rather than sharing bandwidth like Ethernet, token ring and other LANs, ATM uses a switching technology that offers a dedicated connection between nodes. Using a 53 byte "cell" (containing 48 bytes of data and 5 bytes of header) of fixed-size rather than variable-size frames, ATM offers scalability to operate at speeds ranging from 1Mbps to 1.2Gbps.

A common backbone implementation for ATM in an existing LAN will involve sending LAN data through a router to an ATM switch. The data is then sent over the ATM network. On the receiving end, ATM cells are converted back to LAN data frames.

ATM offers a scaleable architecture for both topology and speed. Because ATM is based on switches, additional switches can be added to accommodate increased network demand. Since ATM is based on fixed-size cells, it provides for deterministic operation, allowing for operation of time-critical applications like voice and multimedia.

ATM is independent of upper layer network protocols, allowing it to reside within current network architectures. This will ease the migration path from existing technologies to the higher performance promised by ATM. [Ref. 9]

a. ATM Limiting Factors

ATM is limited by very high costs for switching. Network adapters currently cost $1,000 to $4,000, and switches cost between $5,000 and $12,000. Prices are expected to drop as the technology matures, but it will remain expensive relative to other desktop oriented high-speed solutions.

For LAN environments, ATM suffers from higher overhead than other high-speed options. For medium to large data files, ATM is less efficient than other protocols like 100BASE-T or 100VG-AnyLAN developed specifically for desktop operation.

ATM standards are still under development and given its high costs and evolving implementation schemes, the technology is unlikely to see widespread LAN use until 1997. [Ref. 9]

ATM is best suited for wide area connectivity requirements, campus networks, and backbone operations. Connectivity to the backbone will commonly be performed via routers, although some users' requirements will be best met by direct connection to a file server.

III. HOW TO BUILD A LAN

A network is a requirement if a company wants to maintain its competive stance. But the problem is that networking technology is evolving so rapidly and becoming so complicated that companies are continually playing catch-up with technology. When a company pursues cutting edge technologies it always assumes the risk of failure and high cost. So building a cost-effective, competitive and expandable network to support organizations is the focus of this chapter. Before beginning the design two condition must be true. The first is that the appropriate budget is available during the development time frame and the second is that adequate personnel and expertise are available to support the operation or training plan.

A. DESIGN

Network design plans have several different approaches. The logical approach process steps are as follows: [Ref. 10, p. 235]

1. Interpret Organization Strategic Plans and Setting Network Goals

An organization has its top level objectives and strategy. The manager should translate the organization strategy into the network plan. The network plan has short and long terms goals. Because networks technology is continually evolving, there cannot be a one-time investment that will keep an organization competitive. On the other hand, the leading edge technologies of networking are always combined with risk that is the result of interoperability and integrity issues .

Short term goals should focus on mission critical functionality to support organizational operations. The time frame for short term plans is 2~3 years. The network's growth and its plans should match the organization's development and the emerging network technologies.

Long terms goals address enterprise integration, future growth, and improving quality of service. The time frame for long term plans can be 10~15 years. Long and short-terms should be continually reviewed and adjusted over time.

2. Review Current Environment

Environment includes how functions are performed in departments, how the data or information flows and is processed in the organization, and how the organization accesses outside resources.

Analyze organizational resources for what the organization has and does not have. Determine what resources need to be shared with other organizations. Make outsourcing decisions consistent with resources. Ascertain what strengths and weaknesses an organization possesses. Identify any potential bottlenecks of information flow within the organization.

The designer should investigate and review the organization architecture, analyze the message and traffic flow and survey and interview the people.

Perform these tasks, if the original network and organization layout at hand would be useful.

3. Define Requirement

The data source for requirements comes mainly from networks users. The requirements typically are the transmission bandwidth at each link or node, response time, availability for resource accessing, data flow refining (if necessary), service quality for different applications, reliability (up time) of networking management, and security features.

The requirements must be stated as clearly as possible and translate to quantitative figures. An example of quantitative requirement would be: The network operations' reliability should be 99.9 percent, or a remote query will take 20 seconds or less to return a result.

All the requirements should be prioritized into three levels, must have, desirable to have and nice to have. Implement these different ranks according to critical functions and the budget available. [Ref. 1, p. 317]

4. Forecast Demand

Forecasting demand is important because it largely determines the size, topology, and service provided by the network. The factors of developing a forecast include; the number of network access lines, traffic, service, interests for the organization, and emerging new applications. From the organization historical data and market research one can easily find the trends and potential new network service to be provided. Combining the forecast demands, the requirements and the goals that have been developed in previous steps, the network functions and capabilities required can then be developed.

5. Evaluate and Select Products

The network products evaluation and selections is a complex processing. There are hundreds of vendors and more than ten times that number of products and variation to choose from. Besides the networks technology is evolving and the network design will possibly be supported by multiple vendors.

To fulfill this step, the designer should coordinate with the technical group that specified the required capability or new products and conduct trials on new equipment. [Ref. 10, p. 241]

Products information collection may be through internet survey, trade shows, and from key vendors.

Selection is based on a comparison of cost and capabilities. Yet there are other important considerations. For example, whether the components are in compliance with international standards, are the vendors independent, interoperability, compatibility with legacy devices, easy to use and manage, and an allowance for future growth.

Network components are rarely supplied by a single vendor. The designer should ensure that each key technical area has two or three vendors for competitive pricing.

The existing components cannot be left out of the design considerations. The components that are to be replaced may still be reusable somewhere else.

6. Economic Study

Economic studies support the proposal of evolving network as the best of the other alternatives. Normally, the cost-benefit analysis are performed through the system life cycle which starts with network planning, and continues to the stage of maintenance and management. The system life cost includes hardware, software, circuit, personnel and training.

Network hardware lifetime is normally three to five years due to the technical obsolescence. One way to analyze cost and benefit is using net present value (NPV) and pay-back period. [Ref. 11, p. 670] but depreciation analysis is a suspect tool in a highly competitive industry like computers and networking.

The most difficult cost to calculate is the circuit cost. There are various tariffs imposed by the telephone companies. Parameters include kind and length of leased lines, traffic volume, time of use, etc. [Ref. 1, p. 351]

The possible benefit includes cost reductions, revenue and intangible benefit. See the cost/benefit categories in Appendix D [Ref. 1, p. 350].

The analysis should perform an accurate job in translating cost and benefit into dollar value to provide for easier justification.

B. IMPLEMENTATION CONSIDERATIONS

1. Schedule Jobs

Implementation involves hardware, software, communication circuits, network management facility, people and training, and written procedures for network operations. There should be a detailed implementation plan to enable a smooth implementation process that interferes or interrupts the organization work as little as possible. For this task to be done properly, computer aids such as Program Evaluation Review Technique (PERT) should be applied.

Experience has shown that the lead times to order components should be taken into account for the development of an implementation schedule. In many cases the items cannot be obtained or delivered at once. Hardware and software must be tested individually before

deployments or installations. Methods for an implement may be an abrupt cut over, chronologically, in predetermined phases, or pilot operation.

The network management and test center is the central control point in the network. This group must be in operation before the network is cut over to an operational status. [Ref. 1, p. 365]

It is recommended that network personnel and the administrator be involved in the processing of implementation. This will give them the opportunity to learn and familiarize themselves with the new environment.

2. Cabling

Good cabling plan can minimize the probability of physical transmission problems. According to statistics 70 percent of the faults in networks are the result of inappropriate cabling. If the designer does not pay attention to the cabling issue it may be the seed of future faults. For example, when using low quality cable, it is highly subject to interference and errors will occur. The messages must be retransmitted which increases the normal traffic load, thus the entire network throughput is downgraded. Cabling tasks often involve several departments, replacing the cable is time consuming and inconvenient work. Proper labeling for cable cannot be overemphasized. Improperly labeled or unlabeled cables are every network manager's nightmare. Each cable should be clearly labeled at both ends, and documented to save time and grief later. Cable distance should also be documented and is valuable information in determining the network layout immediately or in the future.

Using UTP Cat 5 indoor and fiber-optic cable outdoor is recommended. Cat5 can be utilized by 100BASE-T, 100VG, FDDI as well as 10BASE-T.

Using structured wire system is not only an easy way to implement but also to manage the network implementation. Another benefit is that it is easy to upgrade the network to meet the future needs. Normally the length of a drop is less than 100 meters.

To meet future applications and bandwidth requirements fiber-optic is the primary media. Wiring an extra number of cables and putting extra 4-inch PVC pipes in while digging the trench will save a lot for network's future growth.

3. Reviews

The easiest activity to skip or overlook is the evaluation of the operating network. After ensuring that the network is properly operated, an evaluation should be conducted. The evaluation serves two purposes: Evaluate the network system which was developed, and evaluate network system development procedures to determine how the project may be improved. [Ref. 1, p. 365] Note that evaluation is the first step to continuing network management over its life cycle.

The network operational feedback come from all the users, network operators and managers. It is important to review users complaints, management complaints, network management trouble reports, network efficiency report, an evaluation of statistic such as traffic load, peak time, volume and error rate of each transmission link, and recommendations. Also it should include a critic comparing the original design's goals and requirements to determine if the design was successfully implemented.

IV. DESIGN EXAMPLE: CHINESE MILITARY SCHOOL NETWORK

A development project for the Chinese military schools campus networks has been proposed at the end of 1994. The Defense Information Management Center tasked Choug-Cheng Instituted of Technology to produce a proposal Chinese military academies networks. The proposal is a result of that tasking and is meant to be a general purpose network and a boiler plate for each school's implementation [Ref. 12]. Basically, the purpose of the project was to provide guidance for the construction of a network for education and administration in the military schools. Network technologies are advancing so fast that the proposal includes legacy equipment that may now be obsolete.

Because this proposal is the initiative for the Chinese military schools to establish a network, and the proposal will also serve as a recommendation for the network infrastructures at Chinese military schools, it should be carefully considered and reexamined to ensure that it represents a good solution for these institutions in light of the current LAN technology. [Ref. 12]

In this chapter the Chinese military school's proposal will be used as an example of redesign. An examination is made of the basic proposal for Chinese military schools and a revised model will be build to illustrate a simplified design for the network. In the following chapter, this new design is evolved through an enhanced model to an advanced model to demonstrate the evolution of the LAN.

A. CURRENT APPROACH

1. The Environment

The Chinese military schools which have an average of approximately 800 students could have 200 to 400 concurrent users including faculty and administration. There are seven military academies in the ROC. They are undergraduate schools specializing in military education. These schools have nearly identical facilities and they are administered by the same command.

Currently, half of the computers are 486 and Pentium type processors, but most run stand alone applications. Most schools have a legacy mainframe which is used by the students and the school administration.

Generally, the school does not run mission-critical operations but focuses on educational and administrative activities.

2. The Basic Model

The 1994 proposal has a potential pitfall in that the design has a router-centric structure which has much less network throughput than a switch-based structure. This potential pitfall exists because the latency of a router is greater than the switch. With the emergence of the new switch technology, the router's role is delegated to serving as networks firewall and an access to WAN, which is the original intended use of routers.

In the basic model of the proposal (See Figure 6), there is a router in the center of the network topology. In this structure each node that requires access to a shared resource

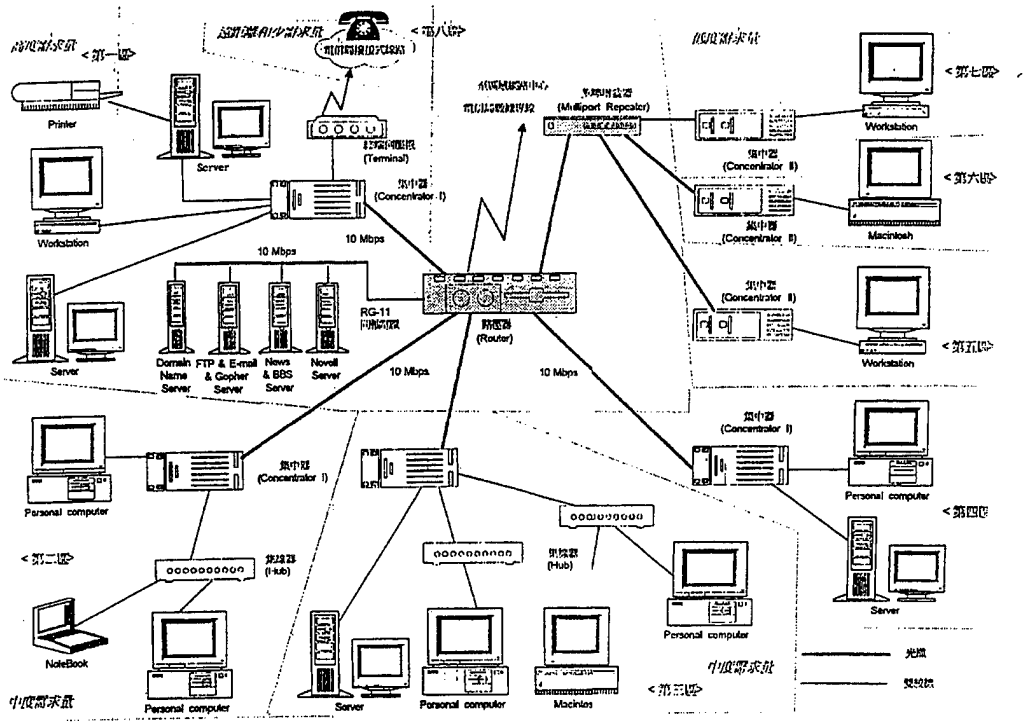

Figure 6. Basic Model of the Proposal

must go through the router. There are several types of computers existing in this model including MAC, PC and workstation (UNIX). In a non-research institute environment, typically the military school, is unnecessary to have those diverse computers. The common servers have a thick coax cable which is more difficult to implement and manage than other types of media. The only benefit of this router-based layout is that it divides a large broadcast domain into several smaller ones, reducing the chance of broadcast storm. But in a 200 to 400 users size networks, generally a broadcast storm is not a problem.

B. REVISED BASIC MODEL

The revised basic model (See Figure 7) takes another approach due to the arrival of new switching technology. The design description is as follows:

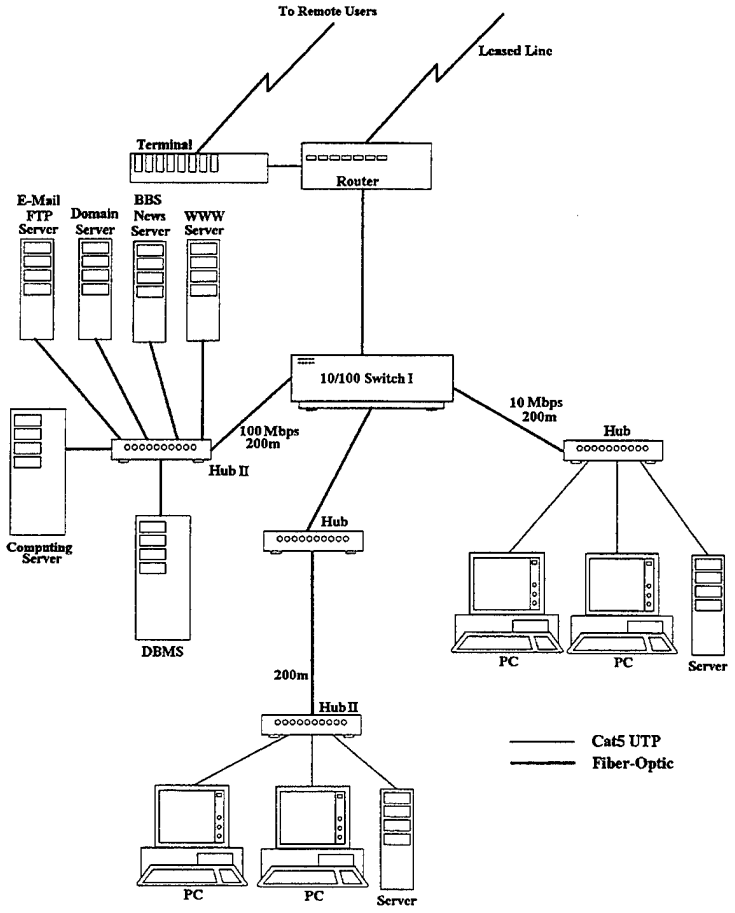

Figure 7. Revised Model

1. The 10/100 Switch sit in the center of the network while the router becomes an edge device providing only firewall and WAN access.

2. The 10/100 Switch has 12 of 10Mbps ports and an 100Mbps port. Each 10Mbps port links to a hub which can downlink up to 24 shared users and servers.

3. The 100Mbps port is reserved for all common servers.

4. The wiring from the center or core switch to all hubs is 200 meters of fiber-optic cable. The wiring which used to connect the users and local servers from a hub is 100 meters, Cat5 UTP cable, hub-to-hub links is 200 fiber-optic meters.

5. The remote user access to campus network is via the terminal.

6. The Switch features power redundant and resilient links.

7. Note that there is two generations hub in this model which is compliance with IEEE Ethernet architecture rules.

C. REASONS FOR REVISING THE BASIC MODEL

According to the result of tests [Ref. 13] the 10/100 Switching Ethernet is much superior to router collapsed backbone and FDDI. In a client/ server query test, the router can support only 50 concurrent users while switch can support up to 150 users. The switch delivers nearly 50 percent better network response time for local traffic (See Figure 8). Of interest is the FDDI which can support 1300 user but the FDDI response time is even worse then that of the router. In an imaging groupware application test, the router is supporting barely 20 users, while the switch can support up to 300 users. The difference in the response time is even greater than that for the switch (24 seconds) comparing to router (44 seconds). The FDDI ranks similarly as in the previous test (See Figure 9). [Ref. 13]

Without translating the delay and throughput of these application tests into dollars, obviously the network planner would avoid the router and the FDDI and choose the switching technology. In the revised model the most important consideration is the cabling, the specific media and its length is deployed to ensure that it meets the most limited network architecture topology rules, the 100BASE-T. In other words, room is left for the networks future growth without the need to recable.

D. THE CAPACITY OF REVISED MODEL

Based on concurrent users in the range of 200 to 400 or a mid-size LAN, and the results of the tests discussed in the previous section, the revised model will have adequate capacity to support the schools' operation.

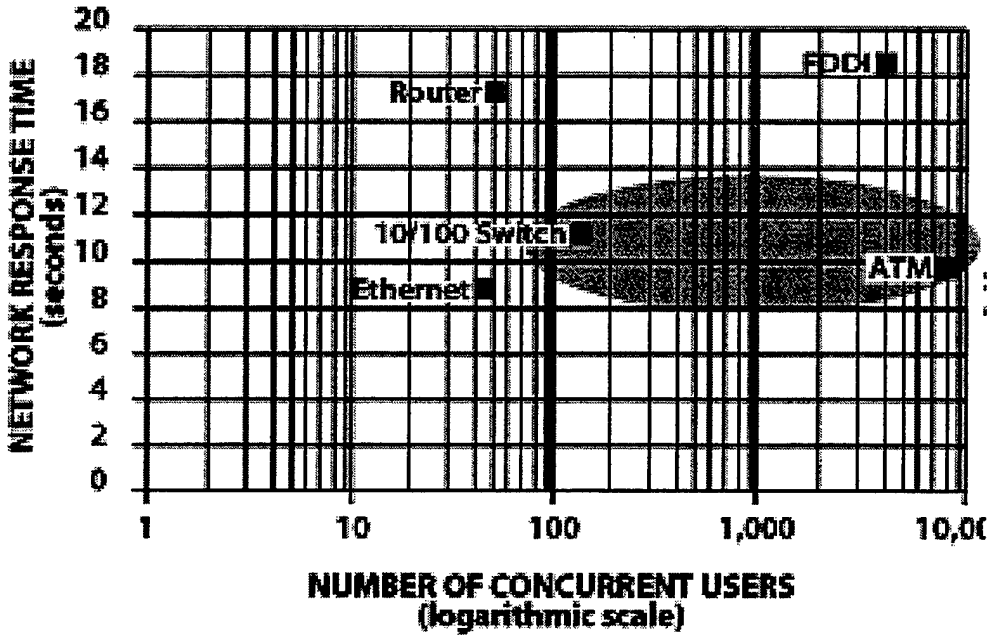

Figure 8. Client/Server Query Correlation Analysis

With 12 10Mbps ports and one 100Mbps ports, the 10/100 switch can adequately support two levels of users. This would be a group numbering 20 to 200. With a simple calculation and with a total of 11, 10Mbps ports, the revised model will support up to 400 users, 200 with slow shares (can be made available to the learning center) and 200 with fast shares.

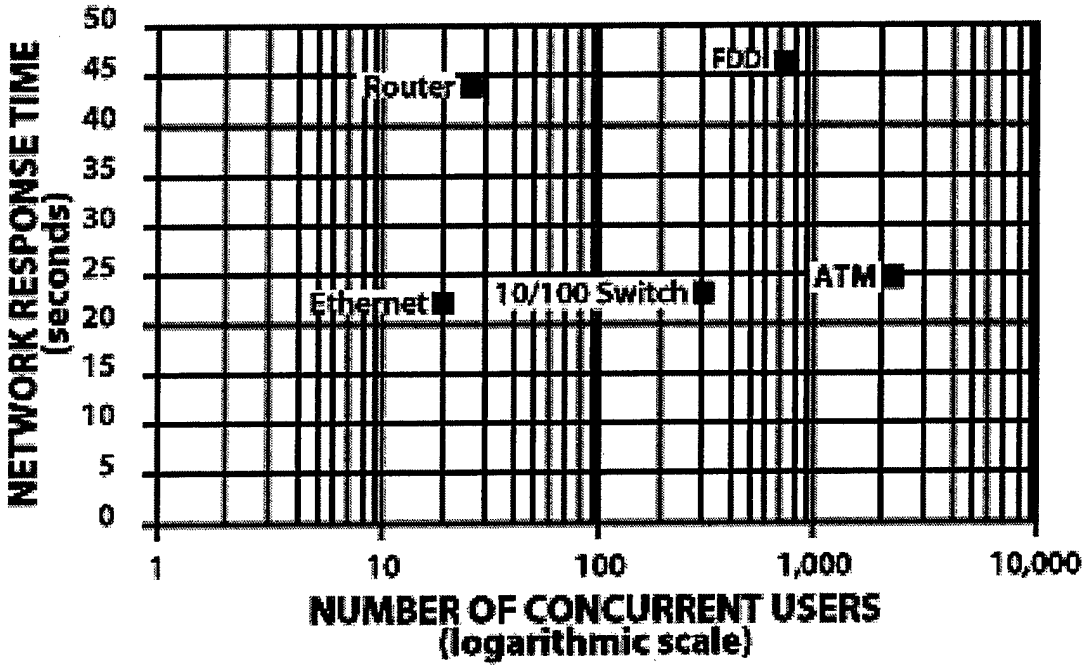

Figure 9. Imaging Groupware Correlation Analysis

V. LAN MIGRATION

With both communication and computer technologies evolving and their combined pressure on LAN growth, the network manager's responsibility is to design a path of LAN migration in order to provide appropriate supports for organization operations.

A. ENHANCED MODEL

As the number of users increase and new client-server applications emerge, the LAN will be required to provide more horsepower for desktop systems and servers. This model continues the previous chapter's revised model, that provides a smooth path of network migration. The purpose of the design will be to increase the bandwidth to accommodate more users and more sophisticated software.

1. Design

This design will fully utilize the advantages of packet-switch technology.

- A new investment is made in a 24 ports 10/100 Switch set in the previous switches position. The new switch is connected to the previous 12 ports Switch using its 100Mbps port, and link to router with its 10M port.
- The design will continue to employ the same cabling method to avoid recabling in the future.
- The common servers such as BBS, News which original are linked to the old switch and are directly connect to the new switch's 10M ports.
- The combined switches provide 34-ports that are available for user groups. If each of the user groups have 20 shares of the subnet, than the maximum population the LAN can support could be as high as 680 users (not to include the local workgroups servers). This design will extend the number of 10M sharing group to support 300 users with 15 ports, upgrade some nodes (up to 18 available) for a 10M dedicated bandwidth by connecting directly to the switches (the remaining port is still available to the learning center).

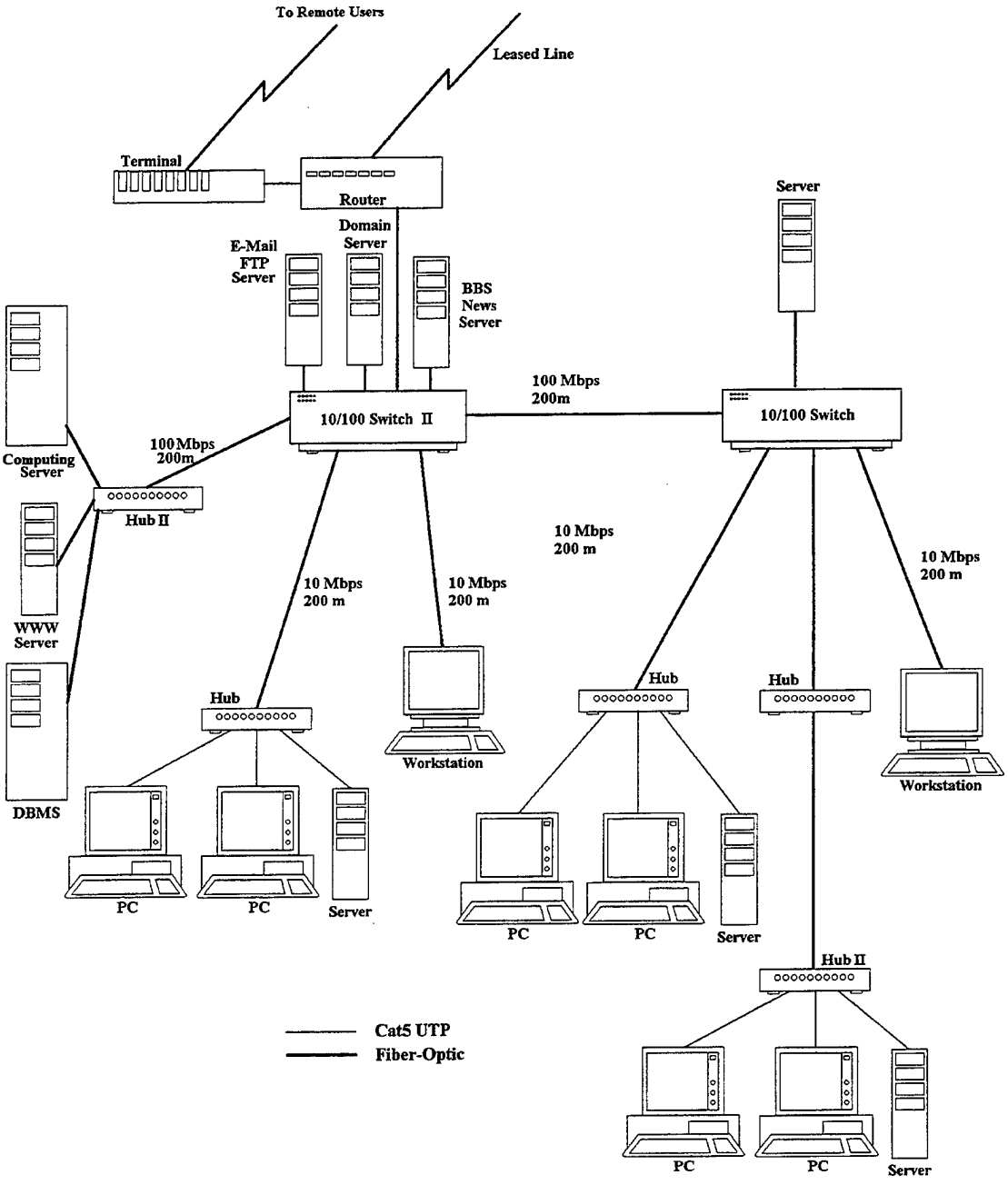

Figure 10. Enhanced Model

2. The Benefits of the Enhanced Model

- The new switch leverages the existing system to support more user and provide for higher performance, greater bandwidth and fulfill increased demand from the users.
- Management is simple in an Ethernet-only environment, implement the switch is simply plug and play. Most of the devices do not need to be moved.
- As Web technology matures the organization can take full advantage of the intranet applications within organization by providing high efficient transmission.
- Has the capabilities of Virtual LAN to create logic usergroup for ease of management.

B. ADVANCED MODEL

As organizations become increasingly dependent on information exchange, applications become more network-centric and reliance of the organization on the network grows. Centralized resources, new classes of applications, new usage paradigms, changing traffic flows, more connected users and more powerful computing platforms all must be taking into account for the network design. The design must increase the capacity and efficiency of networking to meet the ever growing users demands.

1. Design

According to the presentation in Chapter IV, adopting to Fast Ethernet is a rational solution for the design. So, the advance model has one Fast Switch and three 24 ports 10/100 switch which are added to the previous system.

- The Fast Switch is implemented at a new location setting in the traffic center of the network. It reaches out to all the 24 ports Switches and the two Fast Hub with it's 100Mbps ports with 400m links.
- A new multimedia server is sharing 100Mbps links with the computing server at first level of Fast Switching hierarchy.

- The WWW and the DBMS are reconfigured onto a 100Mbps links at first level of Fast Switching hierarchy.

- The high performance workstations and servers share the 100 megabyte speed at the first level of the LAN. The max nodes that can be supported is up to 36, but initially the design only implements 8 of high performance workstations.

- The totally 10Mbps ports are 108 (three are reserved for BBS, DN, E-mail server). This would give the network abundant capacity to feed users demands. Fifteen workgroups (support 300 users) and 93 dedicated users are designed. The learning center slow sharing nodes all would be upgraded.

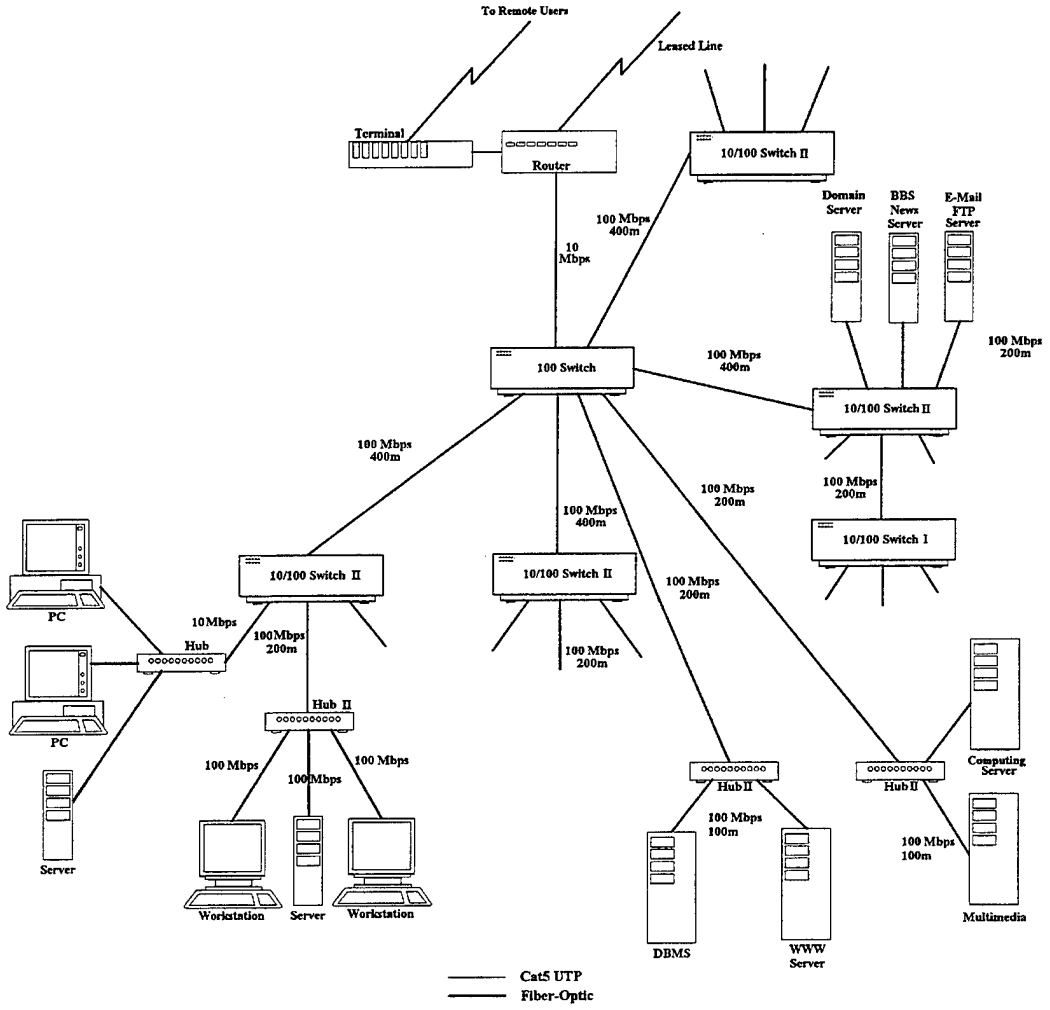

Figure 11. Advanced Model

2. Benefits of Advanced Model

- In this hybrid model, the network provides an easily, tuned, troubleshot and scaled structure.
- The design provides a near-term migration to high-speed workgroup connection without interrupting network operation.
- The advanced model is a cost-effective migration that maximizes the use of the existing network infrastructure.
- Nearly no additional training and expertise are required for network administration. Because the technology is the same, but more capable.
- High performance workstations can enjoy the high speed transmission advantage by only replacing their existing adapter with a 100Mbps adapter.

C. SUMMARY

The enhanced and advanced model designs take full advantage of switching characteristics by forming clusters of the switches and users. The switches are highly scaleable, have high performance, are easy to manage, and are low cost. Only difference between the designs is that the advanced model has higher horsepower.

The common servers from the figures look as if they are separated, indeed, they are concentrated in a single operation center. The servers are directly linked to the centric Switch. A server for a typical workgroup may be built as close to the users as possible to eliminate the unncessary traffic between network devices. In these two models, the device plug-and-play design and abundant bandwidth capacity configuration give network manager great flexibility to tune the network operation, meet the user demands, and control the traffic. The switches are Virtual LAN capable. With these switches, the manager can create logical workgroups that are easily added, removed, or isolated, and confine the broadcast domain to the logical workgroup boundary.

This path of the LAN migration is smooth, nearly no transition time and additional expertise are required. With the embedded VLAN, it is ready to adapt to the future and ATM.

VI. CONCLUSION AND RECOMMENDATION

A. CONCLUSION

1. Knowledgeable and Sustainable Organizational Goal

Networking technologies are rapidly advancing and network architecture has many alternatives. Network managers need to be sure that they are not led into a maze. The purpose of networking is to support organization's business functions and achieve the organization's goals of providing better service and increased productivity.

Having knowledge of networking and understanding the characteristics of each alternatives, the network manager must understand the organization's strategy and organization environment. The organizational strategy is the starting point for network planning. Only then can the manager follow up the with a logical design. Otherwise the manager will follow the wrong route for an upgrade. For example: The 100VG-AnyLAN is an excellent technology, it's best suited for a mid-size network, real time application, has more security feature. But the designer may not choose it, not just because he risks failure for a lack of vendors that are committed to it, but the core reason is that the designer's network requirements derived from the logic design steps do not show a need for it.

2. Easing the Path of Migration

The challenge of network design is that when pursuing high performance, excellent network response time and manageability, the network should accommodate an easy path for network transition. Millions of dollars have been spent in the legacy system. Network infrastructure include existing networks device, software, expertise, and experience and all are considered organization asset. The new investment should leverage the existing network infrastructure. In Chapter IV and V can be viewed as an example that demonstrates that network planner with diverse technologies available and in a rapidly advancing environment for the design of an optimum solution for the organization. That design not only meets users demands but also has a graceful growth path; low cost, nearly no

additional training and expertise needed, and the resulting network is scaleable and easily expanded.

3. Ready for Change

The advanced model discussed in the previous chapter is VLAN capable and is ready to adopt the future promise of ATM. But in the accelerating world of networking technology, it is difficult to predict what will be the best solution for tomorrow's organization. Some things can be grasped: what are the organizations goals; what are the organization needs. The best philosophy for adjusting to a new situation is to build your network as an open system, multivendor supportable, and market proven so as to ensure a less expensive network and with less risk of failure.

B. RECOMMENDATION

1. Cooperation

Decisions about network design must take into account new applications that the network will serve. When planning a network, application developers and network planners should work closer together and create multidisciplinary teams that work with the users of the network. These teams will help users to understand requirements and leave the users with reasonable expectations of the network.

2. Compromise with Efficiency

The network security must be considered and its importance must be balanced with that of network performance. Organization cannot afford the loss or corruption of valuable data, or a system failure. Education and training will help users to better understand and to comply with network security policies and the continued success of the network will be assured.

APPENDIX A. IBM CABLE SYSTEM

A. TYPE 1

Type 1 cable is shielded twisted-pair (STP), with two pairs of 22-gauge solid wire. It is used for data-quality transmission in IBM's Token Ring network. It can be used for the main ring or to connect lobes (nodes) to multistation attachment units (MAUs), which are wiring centers. Although not required by the specifications, a plenum version is also available, at about twice the cost of the nonplenum cable. Compare Type 1 with Type 6.

B. TYPE 2

Type 2 is a hybrid consisting of four pairs of unshielded 22-gauge solid wire (for voice transmission) and two pairs of shielded 22-gauge solid wire (for data). Although not required by the specifications, a plenum version is also available, at about twice the cost.

C. TYPE 3

Type 3 is unshielded twisted-pair (UTP), with two, three, or four pairs of 22- or 24-gauge solid wire. The pairs have at least two twists per foot. This category requires only voice-grade capabilities, and so may be used as telephone wire for voice transmissions. Type 3 is not recommended for 16 Mbps Token Ring networks.

Although not required by the specifications, a plenum version is also available, at about twice the cost. Type 3 cable is becoming more popular as adapter cable, which is used to connect a node to a MAU. You must use a media filter if you are using Type 3 cable to connect a node to a MAU or if you need to switch between UTP and STP in a Token Ring network. However, you should not mix Type 1 and 3 cable in the same ring. Mixing cable types makes troubleshooting difficult.

Some manufacturers offer higher-quality Type 3 cable for greater reliability. Such cable has more twists per foot, for greater protection against interference. Many vendors recommend that you use Category 4 cable (with 12 twists per foot). This category of cable

costs about 20 percent more than ordinary Type 3 cable, but is rated for higher speeds. The category value represents a classification system for the performance of UTP cable.

D. TYPE 5

Type 5 is fiber-optic cable, with two glass fiber cores, each with a 100-micron diameter and a 140-micron cladding diameter. (IBM also allows the more widely used 62.5/125-micron fiber.)This type is used for the main ring path (the main network cabling) in a Token Ring network to connect MAUs over greater distances or to connect network segments between buildings. Plenum versions of Type 5 cable are available at only a slightly higher cost.

E. TYPE 6

Type 6 is STP cable, with two pairs of 26-gauge stranded wire. This type is commonly used as an adapter cable to connect a node to a MAU. In that type of connection, the PC end of the cable has a male DB-9 or DB-25 connector, and the MAU end has a specially designed IBM data connector. Type 6 cable is also used as a patch cable; for example, to connect MAUs. For this use, the cable has IBM data connectors at each end. Because Type 6 is used mostly for shorter distances, the price per foot tends to be higher than for other cable types.

F. TYPE 8

Type 8 is STP cable, with two pairs of flat, 26-gauge solid wire. This type is specially designed to be run under a carpet, so the wires are flattened. This makes the cable much more prone to signal loss than Type 1 or Type 2 cable; however, the performance of Type 8 cable is adequate for the short distances usually involved in under-the-carpet cabling.

G. TYPE 9

Type 9 is STP cable, with two pairs of 26-gauge solid or stranded wire. This type is covered with a plenum jacket and is designed to be run between floors.

APPENDIX B. TOKEN RING LOBE LENGTH AND RING LENGTH RESTRICTIONS.

The lobe length is the distance between a node and an MAU.

- For Types 1 and 2 cable (both STP), the maximum lobe length is 100 meters.
- For types 6 and 9 (also STP), the maximum lobe length is only about 66 meters.
- For UTP (such as Type 3 cable), the maximum lobe length is 45 meters.

The ring length is the distance between MAUs on the main ring path.

- For Types 1 and 2 cable, the distance between MAUs can be up to 200 meters.
- For Type 3 cable, the distance between MAUs can be up to about 120 meters.
- For Type 6 cable, the distance between MAUs can be up to only about 45 meters, because this type is intended for use as a patch cable.
- Fiber-optic cable segments can be as long as 1 kilometer.

There is also a minimum distance constraint: lobes must be separated by at least 2.5 meters.

APPENDIX C. 100BASE-T TOPOLOGY RULES AND FIGURE

The 100BASE-T standard defines two classes of repeaters, called Class I and Class II repeaters. A collision domain can include at most one Class I or two Class II repeaters. Key topology rules are as follows:

Using two Class II repeaters, the maximum diameter of the collision domain is 205 meters (typically 100m + 5m + 100m).

With just a single Class II repeater in the collision domain, the diameter can be extended to 309 meters using fiber (typically 100m UTP + 209m fiber downlink).

With a single Class I repeater in the collision domain, the diameter can be extended to 261 meters using fiber (typically 100m UTP + 161m fiber downlink).

Connecting from MAC to MAC (switch to switch, or end-station to switch) using half-duplex 100BASE-FX, a 412-meter fiber run is allowed.

For very long distance runs, a nonstandard, full-duplex version of 100BASE-FX can be used to connect two devices over a 2-kilometer distance. The IEEE is currently working on a standard for full duplex, but at this time all full-duplex solutions are proprietary.

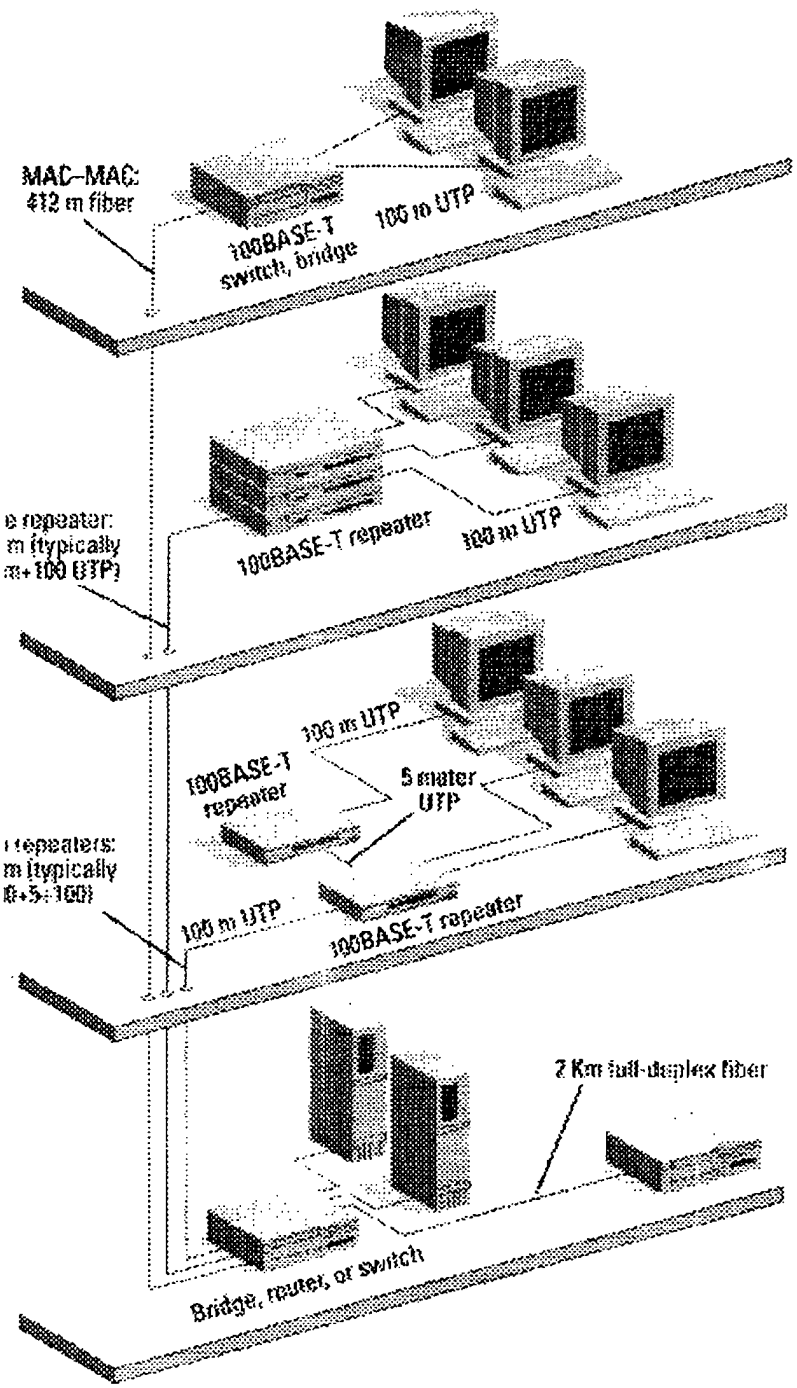

Figure 12. 100BASE-T Topology Rules Illustration

APPENDIX D. COST BENEFIT CATEGORIES

Costs	Benefits
Direct costs • Computer equipment • Communication equipment • Common carrier line charges • Software • Operations personnel costs • File conversion costs • Facilities costs (space, power, air conditioning, storage space, offices, etc.) • Spare parts costs • Hardware maintenance costs • Software maintenance costs • Interaction with vendor and/or development group • Development and performance of acceptance test procedures and parallel operation • Development of documentation • Costs for backup of network in case of failure • Costs of manually performing tests during a system outage • Security and control • Personnel **Indirect costs** • Personnel training • Transformation of operational procedures • Development of support software • Disruption of normal activities • Increased system outage rate during initial operation period • Increase in the number of vendors (impacts fault detection and correction because of "finger pointing")	**Direct and indirect cost reductions** • Elimination of clerical personnel and/or manual operations • Reduction of inventories, manufacturing, sales, operations, and management costs • Effective cost reduction, for example, less spoilage or waste, elimination of obsolete materials, and less pilferage • Distribution of resources across demand for service **Revenue increases** • Increased sales because of better responsiveness • Improved services • Faster processing of operations **Intangible benefits** • Smoothing of operational flows • Reduced volume of paper produced and handled • Rise in level of service quality and performance • Expansion capability • Improved decision process by provision of faster access to information • Ability to meet the competition • Future cost avoidance • Positive effect on other classes of investments or resources such as better utilization of money, more efficient use of floor space or personnel, and so forth • Improved employee morale • Keeping technical employees • Faster decision making

Table 4. Cost Benefit Categories

APPENDIX E. OSI MODEL

1. Application Layer. This topmost layer is responsible for giving applications access to the network. The layer contains application service elements to support application process such as file transfer, electronic-mail, remote file access, virtual terminal, etc.

2. Presentation Layer. The presentation layer provides the data format translation capability needed in a multivendor environment to mask the difference of varying data formats. Function such as data conversion, data compression, data encryption, and expansion of graphics commands.

3. Session Layer. Set up and manages dialogs between communicating users. Controls the use of the basic communication facilities provided by the transport layer.

4. Transport Layer. Provides end-to-end transport of data between communication users, including error recovery and flow control. There are three types of subnet service are distinguished: Type A is very reliable, connection-oriented service; Type B is unreliable, connection-oriented service; Type C is unreliable, connectionless service [Ref. 4, p. 732]. The services needed at this layer depend on what the subnet layers do. The more work the subnet layers do, the less the transport layer must do.

5. Network Layer. Provides the means to establish, maintain, and terminate network on communication. It also translates address from hardware to network and finds a route within and between individual networks.

6. Data-Link Layer. Concerned with procedures and protocols for operating the communication lines. Detects and corrects message errors. Data-Link layer is subdivided into the Logical Link Control (LLC) sublayer and the Media Access Control (MAC) sublayer. Logical Link Control is for data link level transmission control, including end-node addressing and error checking. Media Access Control is a media-specific, access-control protocol such as CSMA/CD, Token Ring , etc.

7. Physical Layer. The physical is the lowest layer in the OSI Model. Deals with physical means of sending data over media. The mechanical, electrical properties of the transmission medium are defined at this layer including the type of cable and connectors used, the pin assignments for the cable, format for the electrical signals.

LIST OF REFERENCES

1. Fitzgerald, Jerry, *Business Data Communication*, Fourth Edition, New York: John Wiley & Sons, 1993.

2. Chellis, James, *The CNE-4 Study Guide*, San Francisco: Network Press, 1996.

3. Stallings, William, *Data and Computer Communication*, Fourth Edition, New York: MacMillan Publishing Company, 1994.

4. Feibel, Werner, *Novell's Complete Encyclopedia of Networking*, San Jose, California: Novell Press, 1995.

5. McClain, Gray R. ed., *Handbook of Networking & Connectivity*, Boston: AP Professional, 1994.

6. 96, Chuck Semeria, Switches and Routers Working Together to Build Scaleable Networks http://www.3com.com/0files/nettechs/papers/swrt.html

7. 100BASE-T Fast Ethernet, 10http:// www.3com.com/ 0files/ strategy /fasteth.html #topology

8. http://www.io.com/~richardr/vg/vgfaq.htm#WhoHasToken

9. http://www.tci.com/papers/hispee5.html

10. Aidarous, Salah and Thomas Plevyak, eds., *Telecommunication Network Management into the 21st Century*, Piscataway, New Jersey: IEEE Press, 1993.

11. Garrison, Ray H., and Eric W. Noreen, *Managerial Accounting*, Boston: Irwin, 1994.

12. Chinese Military Schools campus backbone research, 1994.

13. Bay Network, Inc., http://www.baynetworks.com/products/papers/wp-network design.html.

14. http://www.3com/.files/nottechr/fiveteth/100 migration.

INITIAL DISTRIBUTION LIST

		No. Copies
1.	Defense Technical Information Center 8725 John J. Kingman Rd., STE 0944 Ft. Belvoir, VA 22060-6218	2
2.	Dudley Knox Library Naval Postgraduate School 411 Dyer Rd. Monterey, California 93943-5101	2
3.	Professor Suresh Sridhar Code SM/SS Naval Postgraduate School Monterey, California 93943-5101	1
4.	Professor Rex Buddenberg Code SM/Bu Naval Postgraduate School Monterey, California 93943-5101	1
5.	Professor Doug Brinkley Code SM/Bi Naval Postgraduate School Monterey, California 93943-5101	1
6.	Ta Hsing # 9 Lane 28, Chiu-Chang St, Nan-Tze Zone, Kaohsiung, Taiwan,ROC	3